MoGua

搜狗输入法TV版 1.1.97.2009111724.APK 分析报告

APP名称:	搜狗输入法TV版

包名:	com.sohu.inputmethod.sogou.tv
域名线索:	20条
URL线索:	11条
邮箱线索:	0条
分析日期:	2024年10月16日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 搜狗输入法TV版.apk
文件大小: 25.79MB
MD5值: c11fdd975bdd759f0ee9198a0bc5fada
SHA1值: 118cfb4370c739d1a78b792174638152694cc2ea
SHA256值: ddb69597259cbb9d0bcd71780df13d6856982fb132bde9179d5722061b116cb5

APP 信息

App名称: 搜狗输入法TV版
包名: com.sohu.inputmethod.sogou.tv
主活动Activity: com.sohu.inputmethod.sogou.SogouIMESettingsLauncher
安卓版本名称: 1.1.97.2009111724
安卓版本: 508

域名线索

域名	服务器信息
talk.speech.sogou.com	没有服务器地理信息.
lh3-dz.googleusercontent.com	**IP**: 142.250.217.97 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
connectivitycheck.gstatic.com	**IP**: 203.208.50.66 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

github.com	**IP**: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
ping.android.shouji.sogou.com	**IP**: 116.130.224.118 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
test.speech.sogou.com	没有服务器地理信息.
127.0.0.1	**IP**: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
ltalk.speech.sogou.com	**IP**: 220.194.117.245 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
shouji.sogou.com	**IP**: 220.194.117.245 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
	IP: 142.250.217.97 **所属国家**: United States of America

googlehosted.l.googleusercontent.com	**地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
lh3.googleusercontent.com	IP: 142.250.217.97 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
online.speech.sogou.com	没有服务器地理信息.
v2.get.sogou.com	IP: 123.125.0.146 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
schemas.android.com	没有服务器地理信息.
speech.sogou.com	IP: 220.194.117.245 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
www.gstatic.com	IP: 203.208.50.98 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
	IP: 74.125.197.82

android.googlesource.com	**所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
srv.android.shouji.sogou.com	**IP**: 116.130.224.118 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
media.tenor.com	**IP**: 182.50.139.56 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
c.tenor.com	**IP**: 128.242.240.180 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903

URL线索

URL信息	Url所在文件
http://online.speech.sogou.com/index.cgi	defpackage/Sr.java
http://speech.sogou.com/index.cgi	defpackage/Sr.java

http://test.speech.sogou.com/index.twcgi	defpackage/Sr.java
http://talk.speech.sogou.com/index.cgi	defpackage/Sr.java
http://test.speech.sogou.com/index.lt	defpackage/Sr.java
http://ltalk.speech.sogou.com/index.lt	defpackage/Sr.java
http://schemas.android.com/apk/res/android	defpackage/C0153Ub.java
http://srv.android.shouji.sogou.com/v1/pingback/kpi2	defpackage/C0272cA.java
http://ping.android.shouji.sogou.com/alive.gif	defpackage/Nx.java
http://ping.android.shouji.sogou.com/androidappalive.gif	defpackage/Nx.java
http://ping.android.shouji.sogou.com/androidinputalive.gif	defpackage/Nx.java
https://github.com/TooTallNate/Java-WebSocket/wiki/Lost-connection-detection	defpackage/_C.java
http://v2.get.sogou.com/q	defpackage/Kz.java
http://shouji.sogou.com/web_ime/mobile.php?	defpackage/C0799rF.java
http://v2.get.sogou.com/q	defpackage/Lz.java
http://srv.android.shouji.sogou.com/v1/config/netswitch	com/sohu/inputmethod/sogou/receiver/UpdateReceiver.java
http://shouji.sogou.com/wap/?c=web&a=goto&id=82	摸瓜V1引擎
https://android.googlesource.com/toolchain/clang	摸瓜V3引擎
lh3-dz.googleusercontent.com	摸瓜V3引擎
connectivitycheck.gstatic.com	摸瓜V3引擎

growth-pa.googleapis.com	摸瓜V3引擎
http://schemas.android.com/aapt	摸瓜V3引擎
android.googleapis.com	摸瓜V3引擎
http://schemas.android.com/apk/res/android	摸瓜V3引擎
http://schemas.android.com/apk/res-auto	摸瓜V3引擎
gmscompliance-pa.googleapis.com	摸瓜V3引擎
play.googleapis.com	摸瓜V3引擎
https://android.googlesource.com/toolchain/llvm	摸瓜V3引擎
http://127.0.0.1:8080/cmsogou.comhttp://127.0.0.1:8080/sohusohu.comsogo.come764b0ca3498cc7d	摸瓜V3引擎
www.googleapis.com	摸瓜V3引擎
googlehosted.l.googleusercontent.com	摸瓜V3引擎
http://schemas.android.com/apk/res/android00launcher.home.preference.SogouCheckBoxPreference	摸瓜V3引擎
lh3.googleusercontent.com	摸瓜V3引擎
http://schemas.android.com/apk/res/android-- launcher.home.preference.RadioGroupPreference&&launcher.	摸瓜V3引擎
www.gstatic.com	摸瓜V3引擎
http://srv.android.shouji.sogou.com/v1/config/netswitch	摸瓜V3引擎
firebaseinstallations.googleapis.com	摸瓜V3引擎

media.tenor.com	摸瓜V3引擎
clientservices.googleapis.com	摸瓜V3引擎
infinitedata-pa.googleapis.com	摸瓜V3引擎
instantmessaging-pa.googleapis.com	摸瓜V3引擎
c.tenor.com	摸瓜V3引擎

邮箱线索

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: False
v3 签名: False
找到 1 个唯一证书
主题: C=CN, ST=Beijing, L=Beijing, O=Wireless, OU=Sohu, CN=Sohu Wireless
签名算法: rsassa_pkcs1v15
有效期自: 2009-09-08 03:28:13+00:00
有效期至: 2037-01-24 03:28:13+00:00
发行人: C=CN, ST=Beijing, L=Beijing, O=Wireless, OU=Sohu, CN=Sohu Wireless
序列号: 0x4aa5cf4d
哈希算法: md5
md5值: 15cd0088e2697091f33a2d97da2ea956
sha1值: 3e6bd5f09ce6f728f0841e7edcf0d30ff5648cd9
sha256值: 01cb5a64feb3f6169e9dbe9c4304b1a7fab12c92af6814dd5f9892aabc01f0f3
sha512值: 17654e12e821c47c814d9270f5dcd206377d4bfce5acf2b0968b617c1b6d17b016ffa594b473c59ce6e0a1416e6af2fb53a42277adb358f5f09e79b7af6c16e5

硬编码敏感信息

可能的敏感信息
"guid_private_info" : "启用即表明您同意搜狗输入法的用户协议和隐私政策"
"guid_private_info_privacy_declaration" : "隐私政策"
"guid_private_info_service_declaration" : "用户协议"
"guid_private_info_unio" : "和"
"handwriting_core_key" : "handwriting_core_key"
"privacy_shown_sp_key" : "privacy_shown"

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

此APP的危险动作

向手机申请的权限	是否危险	类型	详细情况
android.permission.READ_PHONE_STATE	危险	读取电话状态和身份	允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.ACCESS_NETWORK_STATE	正常	查看网络状态	允许应用程序查看所有网络的状态
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储
android.permission.READ_EXTERNAL_STORAGE	危险	读取外部存储器内容	允许应用程序从外部存储读取
android.permission.ACCESS_WIFI_STATE	正常	查看Wi-Fi状态	允许应用程序查看有关 Wi-Fi 状态的信息
android.permission.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.WAKE_LOCK	正常	防止手机睡眠	允许应用程序防止手机进入睡眠状态
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器

android.permission.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
android.permission.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人

应用内通信
